

Background of S/MIME

- ❑ **Problems of existing secure e-mail systems**
 - PEM : hard to implement
 - PGP : low security, hard to be compatible with existing e-mailing system
- ❑ **Growth of S/MIME**
 - IETF adopted S/MIME V2 as standard
 - many applications like Outlook(Microsoft), Communicator(Netscape), Eudora(Qualcomm) etc.
 - Many toolkits like S/MIME toolkit (RSA), S/MIME Freeware Library(VDA : J.A. Van Dyke and Association) etc.

RFC822

- ❑ **“Standard for the format of ARPA Internet text message”**
- ❑ **Format for text message via e-mail**
- ❑ **Message = envelop + contents**
 - **env. : whatever information is needed to accomplish transmission and delivery**
 - **con. : compose the object to recipient**
 - **(ex) header line + unrestricted text (body) separate by blank line**
 - **header’s keyword : From, To, Subject, date, message ID etc**

Limitation of SMTP/RFC822

- ❑ can't send binary files
- ❑ can't send 8 bit codes
- ❑ reject mail message over a certain size
- ❑ SMTP gateways translating ASCII to EBCDIC don't use consistent set of mapping
- ❑ non-compatibility with X.400
- ❑ Some implementation problems
 - deletion, addition or reordering of CR and LF
 - Truncating or wrapping lines longer than 76 character

MIME (I)

- **“Multipurpose Internet Mail Extensions”**
 - **rfc2045 MIME part 1 : Format of Internet message bodies**
 - **rfc2046 MIME part 2 : Media types**
 - **rfc2047 MIME part 3 : Message header extensions for Non-ASCII text**
 - **rfc2048 MIME part 4 : Registration procedure**
 - **rfc2049 MIME part 5 : Conformance criteria and examples**

MIME(II)

- ❑ **5 Headers : MIME-version, Content-type, Content-transfer-Encoding, Content-ID, Content-Description**
- ❑ **Can express Multimedia e-mail**
- ❑ **Define Transfer encoding**
- ❑ **Compatible with rfc822**

MIME Content Type

Type	Subtype	Description
Text	Plain	Unformatted text; maybe ASCII or ISO8859
	Enriched	Provides greater format flexibility
Multipart	Mixed	Different part independent,
	Parallel	No order defined same as Mixed
	Alternative	
	Digest	
Message	rfc822	
	Partial	
	External-body	
Image	jpeg	
	gif	
Video	mpeg	
Audio	Basic	
Application	PostScript	
	octet-stream	

MIME transfer encoding

- ❑ **7 bit : short lines of ASCII char.**
- ❑ **8 bit : short lines with non-ASCII char.**
- ❑ **Binary : non-ASCII + SMTP transportability**
- ❑ **quoted-printable**
- ❑ **base64 : radix 64 encoding**
- ❑ **x-token : named nonstandard encoding**

Features of S/MIME

- ❑ **Classification**
 - **S/MIME : RSADSI**
 - **S/MIME v2 : RSADSI + multi-vendor consortium**
 - **S/MIME v3 : IETF + product vendor**
- ❑ **Adding encryption function of MIME-style message**
- ❑ **Use PKCS #7 Cryptographic Message Syntax**
- ❑ **Use X.509 v3.**

Documents of S/MIME

□ V2

- S/MIME v.2 Message Specification (RFC2311)
- S/MIME v.2 Certificate handling (RFC2312)

□ V3

- Cryptographic Message Syntax (draft-ietf-smime-cms)
- S/MIME v.3 Message Specification (draft-ietf-smime-msg)
- S/MIME v.3 Certificate Handling (draft-ietf-smime-cert)
- Enhanced Security Service for S/MIME (draft-ietf-smime-ess)

S/MIME Goals

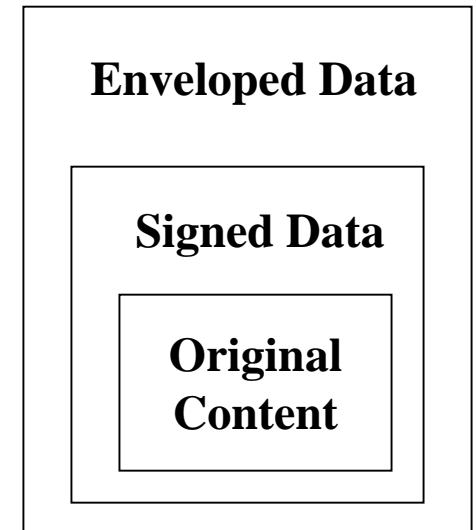
- ❑ **Strong encryption**
- ❑ **Digital signatures**
- ❑ **Ease of use**
- ❑ **Flexibility trust to fit business**
- ❑ **Interoperability**
- ❑ **Exportability**

S/MIME functionality

- ❑ **Enveloped data : encrypted content of any type and encrypted-content encryption key for one or more recipients**
- ❑ **Signed data : digital signature + encrypting with private key + base64 encoding**
- ❑ **Clear-signed data : signed data + base64 encoded digital signature**
- ❑ **Signed and enveloped data : signed-only and encrypted-only nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted**

Message of S/MIME

- ❑ Clear data
- ❑ Signed data
- ❑ Enveloped data
- ❑ Signed and enveloped data



Scalable Trust

- ❑ **Direct Trust**
- ❑ **Cross certification**
- ❑ **(Hierarchical) Certification Authority**

S/MIME Certificate Handling

- ❑ **X.509 CA + PGP's Web of trust**
- ❑ **S/MIME managers and users must configure each client with a list of trusted keys and with CRL**
- ❑ **local responsibility for maintaining certificates to verify incoming signature and to encrypt outgoing message**
- ❑ **UA's role : Key generation, Registration, Certificate storage and retrieval**

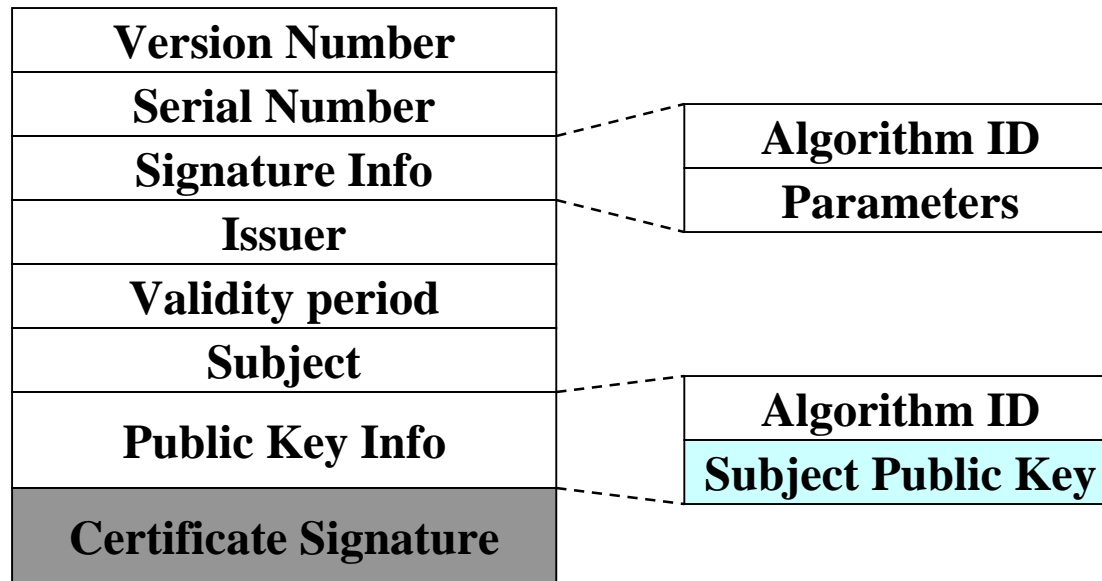
CA service

- ❑ **Verisign**
- ❑ **GTE**
- ❑ **U.S. Postal Service**
- ❑ **KISA**
- ❑ **KT/ Dacom**
- ❑ **3 big parties (EC, banking, security)
etc**

Key storage of S/MIME

- Use certificate

X.509 Certificate Format Ver.3.0



Features of S/MIME v3

- ❑ **Use DSA, DH-PKC**
- ❑ **Use SHA-1**
- ❑ **Signed receipts : signing by receiver's private key of signed message for proof of delivery**
- ❑ **Security labels : access right to original message**
- ❑ **Secure mailing lists : In case of multiple receivers, MLA (Mail List Agent) sends encrypted message per a receiver.**

S/MIME Support

AOL

Banyan

Blue Mountain

CommerceNet EDI Pilot

***ConnectSoft**

***Deming**

***Frontier Technologies**

FTP

GlobalKey

Harbinger

Lotus

Microsoft()**

Netscape

Nortel

Novell

***OpenSoft**

Premenos

Qualcomm()**

SecureWare

Sterling

***Verisign**

*** : Direct Support**

**** : Plug-in**

S/MIME Web page

The screenshot shows a Netscape browser window with the address bar displaying <http://www.rsa.com/smime/>. The page title is "S/MIME Central". The main content area contains a paragraph explaining S/MIME as a specification for secure electronic messaging, created in 1995 to solve the problem of interception and forgery of e-mail. It mentions that S/MIME is short for Secure MIME and is designed to be easily integrated into e-mail and messaging products. It also states that S/MIME builds security on top of the industry standard MIME protocol according to cryptographic standards like PKCS. To the right of the text is an image of a stack of envelopes with "S/MIME ENABLED" stamps. Below the text is another paragraph stating that S/MIME was created using other standards and is likely to be widely implemented. On the right side of the page, there are several navigation links: "S/MIME FAQ", "S/MIME Products", "In The News", "Interoperability Center", and "Developer Resources". At the bottom right, there is a VeriSign logo and a link to "Visit VeriSign's Secure E-Mail Reference Guide to find out how to secure your email with S/MIME."

Forward Reload Home Search Guide Print Security Stop


Bookmarks Netsite: <http://www.rsa.com/smime/>

Print Message Internet Lookup New&Cool

S/MIME Central

S/MIME is a specification for secure electronic messaging. In 1995, several software vendors got together and created S/MIME to solve a very real problem - interception and forgery of e-mail. Protecting sensitive data is a real concern, especially in a world that is becoming increasingly more wired. The goal of S/MIME is to make it easy to secure messages from prying eyes. Since its creation, S/MIME has come a long way.

S/MIME is short for Secure MIME. The specification was designed to be easily integrated into e-mail and messaging products.



S/MIME builds security on top of the industry standard MIME protocol according to an equally important set of cryptographic standards, the Public Key Cryptography Standards (PKCS). The fact that S/MIME was created using other standards is important for something that is likely to be widely implemented.


S/MIME FAQ

S/MIME Products

In The News

Interoperability Center

Developer Resources



Visit [VeriSign's Secure E-Mail Reference Guide](#) to find out how to secure your email with S/MIME.

Comparison of PGP and S/MIME(I)

	PGP 2.6 <i>(Classic)</i>	PGP/MIME <i>(IETF)</i>	PGP 5.0	OpenPGP <i>(IETF)</i>	S/MIME v2	S/MIME v3 <i>(IETF)</i>
Packaging	Special	MIME	Special, MIME	MIME	MIME, Special	MIME, CMS
Signing	(Text in Body)					
Encrypting		Special			PKCS#7	CMS
Records		Special Binary			PKCS#7	CMS
Transport Protection	Special <i>(ASCII Armor)</i>	MIME and Special	Special		MIME, Special	MIME
Selection		Special Binary			PKCS#7	CMS
Algorithms		Special (Web of trust)			X.509	9 v3
Certificate					(PKIX?)	
Session	RSA		ElGamal, RSA	ElGamal	RSA	Diffie-Hellman (X9.42), RSA
Digest	MD5	SHA-1, MD5			SHA-1,	MD-5
Signed	RSA		DSA,	RSA	RSA	DSA, RSA
Encrypt	IDEA		CAST5, IDEA, TripleDES	TripleDES (EDE), IDEA, CAST5	RC2-40, TripleDES	TripleDES (CBC), RC2-40, DES

Description

- ❑ **Signing, Encrypting** : Packaging sections of data and control information into Internet Mail and distinguishing between the sections
- ❑ **Records** : Separating internal information “records” and fields
- ❑ **Transport Protection** : Protection data against vagaries of transport services -- especially email transport -- by adding a layer of data encoding, for example, so that trailing white spaces are not eliminated.
- ❑ **Selection** : Mechanism for specifying choices among algorithms etc.
- ❑ **Certificate** : Associating identifiers with keys and validating the association
- ❑ **Session** : Public key mechanism for exchanging random session keys between correspondents
- ❑ **Digest** : Algorithm(s) for performing data integrity hash calculation
- ❑ **Signed** : Algorithm(s) for encrypting content digest to achieve data authentication
- ❑ **Encrypt** : Algorithm(s) supported for encrypting content data to achieve privacy

Comparison of PGP and S/MIME(II)

Others

Class	PGP	S/MIME
Authentication policy	Distributed authentication	Hierarchical authentication
Key storage	Key ring	Key certificate
Standard	-	IETF
Commercialization	No compatibility test Small products	Compatibility test Many commercial products
Main Usage	Personal	Company, Enterprise